A FAMILY OF EISENSTEIN POLYNOMIALS GENERATING TOTALLY RAMIFIED EXTENSIONS, IDENTIFICATION OF EXTENSIONS AND CONSTRUCTION OF CLASS FIELDS

MAURIZIO MONGE

ABSTRACT. Let K be a local field with finite residue field, we define a normal form for Eisenstein polynomials depending on the choice of a uniformizer π_K and of residue representatives. The isomorphism classes of extensions generated by the polynomials in the family exhaust all totally ramified extensions, and the multiplicity with which each isomorphism class L/K appears is always smaller than the number of conjugates of L over K.

An algorithm to recover the set of all special polynomials generating the extension determined by a general Eisenstein polynomial is described. We also give a criterion to quickly establish that a polynomial generates a different extension from that generated by a set of special polynomials, such criterion does not only depend on the usual distance on the set of Eisenstein polynomials considered by Krasner and others.

We conclude with an algorithm for the construction of the unique special equation determining a totally ramified class field in general degree, given a suitable representation of a group of norms.

1. INTRODUCTION

In this note we show how it is possible to define a normal form for Eisenstein polynomials, which can be used for quickly enumerating totally ramified extensions of a local field, for selecting a special defining polynomial to represent extensions, and for identification of the extensions. Unluckily it doesn't seem possible to produce easily exactly one special polynomial for each isomorphism class of extensions, but we show how to obtain a very restricted set of polynomials generating each extension. The number of special polynomials generating a fixed extension L/K is always smaller that the number of conjugates of L over K, so that each Galois extensions is generated by exactly one polynomial. In fact, the problem of selecting exactly one generating polynomial for each isomorphism class appears to be as hard as that of determining the cardinality of the group of automorphisms of the extension generated by a polynomial.

As shown in [PR01], it is possible to enumerate and identify the extensions generated by Eisenstein polynomials selecting one polynomial for each neighborhood with respect to a suitable distance, and applying Panayi root finding algorithm to collect the polynomials which generate the same extension. The search space can be drastically reduced by just taking into account Eisenstein polynomials in normal form.

Furthermore, for each Eisenstein polynomial generating an extension L/K of degree n there exists a quick way to recover all the special polynomials attached to the extension, which does not require an exhaustive search over the space of

all extensions of degree n of K, not even a search within the set of polynomials generating extensions with fixed ramification data.

Indeed, any Eisenstein polynomial can be put into normal form by applying greedily a reduction algorithm, which however allows some free choices during the reduction. The full set of special polynomials is obtained as the set of all possible outputs of the reduction algorithm, over all possible choices.

We exhibit a criterion for establishing *a priori* that an Eisenstein polynomial $f(T)$ may not be converted to another polynomial $g(T)$ via such a reduction applied greedily, and when $f(T)$ and $g(T)$ are any two Eisenstein polynomials such that one of them is known to generate a Galois extension then the criterion can be used to show that $f(T)$ and $g(T)$ generate non-isomorphic extensions. The criterion takes into account the higher order terms appearing in the p-adic expansion of the coefficients, not just the valuation (or first-order expression) of $f(\pi) - g(\pi)$ for a uniformizer π of an extension L/K of degree n. The criterion established in [Yos11] for totally ramified Galois extensions over $\mathbb{Q}_p$ is also recovered in a more general context.

In the last section we describe an algorithm which allows to construct the unique special Eisenstein polynomial generating a totally ramified class field, given a suitable description of a norm subgroup. In particular, we show that there exists an ordering of the terms appearing in the p-adic expansions of the coefficients which allows to recover all the terms of the special polynomial, by solving inductively linear equations over the residue field. An algorithm for the construction of polynomials generating class field was described in [Pau06] for cyclic extensions, where an extension of degree p^m is constructed inductively by steps of degree p. In our construction an Eisenstein polynomial generating an arbitrary totally ramified class field is constructed directly.

1.1. **Acknowledgements.** We would like to thank Philippe Cassou-Noguès, Ilaria Del Corso, Roberto Dvornicich and Boas Erez for various discussions on this topic, and the Institut de Mathématiques de Bordeaux for hospitality while conceiving this work.

1.2. **Notation.** All local fields will be assumed to have finite residue field, even though most results hold just assuming it to be perfect, and some even in greater generality.

If F is any local field, we denote by $\mathcal{O}_F$ its ring of integers with unique maximal ideal $\mathfrak{p}_F$, and by κ_F the residue field $\mathcal{O}_F/\mathfrak{p}_F$. We denote by v_F the normalized valuation and by e_F the absolute ramification index $v_F(p)$ (if F has characteristic p we will be fine with $e_F = +\infty$).

Let L/K be a separable totally ramified extension of degree n, we denote by $\Gamma = \Gamma(L/K)$ the set of all K-embeddings of L into a fixed separable algebraic closure L^{sep} of L. For $\sigma \in \Gamma(L/K)$ we define

$$i_{L/K}(\sigma) = \min_{x \in \mathcal{O}_L} v_L(\sigma(x)/x - 1),$$

which is also equal to $v_L(\sigma(\pi)/\pi - 1)$ for a uniformizing element $\pi = \pi_L$ generating the maximal ideal $\mathfrak{p}_L$ of $\mathcal{O}_L$. For each real x we set

$$\Gamma_x = \{\sigma \in \Gamma : i_{L/K}(\sigma) \geq x\},$$
$$\Gamma_{x^+} = \{\sigma \in \Gamma : i_{L/K}(\sigma) > x\},$$

our definition is equal to that in [Yam68] and reduces to the classical definition of ramification subgroups of [FV02, Ser79, Del84] for Galois extensions, and differs by a shift by 1 from that used in [Lub81, Hel91].

We say that x is a *ramification break* if $\Gamma_x \supsetneq \Gamma_{x+}$, and let K_x and K_{x+} respectively be the fields fixed by Γ_x and Γ_{x+}.

We put

$$\phi_{L/K}(x) = \frac{1}{n}\int_0^x (\#\Gamma_t)\, dt,$$

and let $\psi_{L/K}$ to be the inverse by composition. Since we only consider totally ramified extensions we restrict both $\phi_{L/K}$ and $\psi_{L/K}$ to $\mathbb{R}^{\geq 0}$.

If L/K is any totally ramified extension of degree n, with k distinct ramification jumps say, we will usually denote with $t_1 < t_2 < \cdots < t_k$ the ramification jumps and with $\gamma_0 > \gamma_1 > \cdots > \gamma_k$ the cardinalities of the corresponding ramification subsets, so that $\gamma_0 = \#\Gamma = n$ and $\gamma_i = \#\Gamma_{t_i^+}$ for $1 \leq i \leq k$. The γ_i are all powers of π, except possibly for $\gamma_0 = n$.

If p^s is the biggest power of p dividing n, for each $0 \leq \ell \leq s$ it will also be convenient putting τ_ℓ to be equal to the smallest real t such that $n\phi_{L/K}(x)$ has slope $\leq p^\ell$ for $x \geq t$, it will be equal to either 0, or some ramification jump t_i. The τ_ℓ are weakly decreasing and exhaust all the lower ramification jumps t_i, and one jump $t_i > 0$ is repeated r times if $(\Gamma_{t_i} : \Gamma_{t_i^+})$ is equal to p^r, so each ramification jump is taken "with its multiplicity" in a suitable sense. It will also be convenient defining

$$\xi_\ell = n\phi_{L/K}(\tau_\ell) - p^\ell \tau_\ell, \qquad \sigma_\ell = n\phi_{L/K}(\tau_\ell),$$

for each $0 \leq \ell \leq s$. Up to a factor n the σ_ℓ are the upper ramification jumps of the extension.

2. REDUCTION ALGORITHM AND THE FAMILY OF REDUCED POLYNOMIALS

Let $f(T) = T^n + f_{n-1}T^{n-1}\ldots f_1 T + f_0$ be a monic Eisenstein polynomial of degree n, let π be a root in a fixed algebraic closure K^{alg} and put $L = K(\pi)$. Then clearly $f(T)$ is the minimal polynomial of π which is a uniformizing element of the extension determined by $f(T)$, and we are interested in understanding how the coefficients of the minimal polynomial of a uniformizer change when π is replaced by another uniformizer $\rho = \pi + \theta\pi^{m+1} + \mathcal{O}(\pi^{m+2})$, for some unit $\theta \in U_K$ and integer $m \geq 1$. Since the computation which follows only depends on θ at the first order, θ may be taken to be a multiplicative representative.

Let us consider the ramification polynomial $\Phi(T) = \pi^{-n}f(\pi T + \pi)$, its Newton polygon is fully described by the lower ramification breaks. For $\alpha \in \mathcal{O}_K$ we can compute a lower bound for the valuation of $\Phi(\alpha)$ as function of $v_L(\alpha)$ starting from the Newton polygon of $\Phi(T)$. The construction produces naturally the *Newton copolygon*, which is essentially the dual convex body of the Newton polygon, and is connected to the Hasse-Herbrand transition function as already observed in [Lub81, Li97]; in such references $f(T + \pi)$ was used instead so the function obtained was slightly different from the classical Hasse-Herbrand defined in [FV02, Ser79].

Indeed, the Newton polygon of the polynomial $\Phi(\pi^m T)$ resulting by the substitution $T \to \pi^m T$ can obtained from the polygon of $\Phi(T)$ moving the points with abscissa x up by $\frac{m}{n}x$. In other words, if $N : [1, n] \to \mathbb{R}$ is the real function describing the polygon of $\Phi(T)$, the polygon of $\Phi(\pi^m T)$ is described by $N(x) + \frac{m}{n}x$.

The function $N(x)$ is convex and piecewise linear, and by the well known properties of Newton polygons the slopes are $-t_k/n, \ldots, -t_1/n$ where $t_1 < t_2 < \cdots < t_k$ are the lower ramification breaks of the extension generated by a root, and it has slope $-t_i/n$ in the interval $[\gamma_i, \gamma_{i-1}]$ where $\gamma_0 > \gamma_1 > \cdots > \gamma_k$ are the cardinalities of the corresponding ramification subsets. We put $t_0 = +\infty$, $t_{k+1} = -\infty$ for convenience.
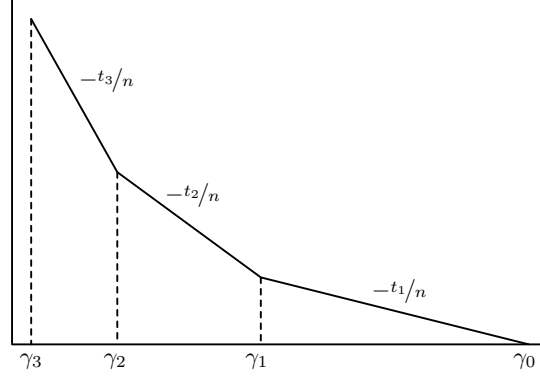
Let's consider the minimum achieved by the function $N(x) + \frac{m}{n}x$ in the interval $[1, n]$, as a function of the real parameter m. It is again a piecewise linear function with slope γ_i/n for $t_i \leq m \leq t_{i+1}$, and we obtain that this minimum value function is exactly the Hasse-Herbrand function $\phi_{L/K}(m)$. Hence this is the smallest valuation (with respect to K) of the coefficients of $\Phi(\pi^m T)$, and $\pi^{-n\phi_{L/K}(m)}$ is the exact power of π such that $\pi^{-n\phi_{L/K}(m)}\Phi(\pi^m T)$ is in $\mathcal{O}_L[T]$ and non trivial modulo $\mathfrak{p}_L$.

Let's define the valuation of a polynomial to be the smallest valuation of the coefficients, we can resume what proved in the following

Proposition 1. *Let $f(T)$ be an Eisenstein polynomial, π a root, $L = K(\pi)$ and $\Phi(T) = \pi^{-n}f(\pi T + \pi)$ its ramification polynomial. Then*

$$v_L(\Phi(\pi^m T)) = n\phi_{L/K}(m).$$

It will also be convenient to deduce an expression for the values $N(p^\ell)$ for each $\ell \geq 0$ such that $p^\ell \mid n$. Starting from p^ℓ the function $N(x)$ has slope $-\tau_\ell/n$, so $N(x) + \frac{\tau_\ell}{n}x$ has infimum equal to $\phi_{L/K}(\tau_\ell)$, which is achieved for $x = p^\ell$ and is also equal to $N(p^\ell) + \frac{\tau_\ell}{n}p^\ell$, so we obtain

$$N(p^\ell) = \phi_{L/K}(\tau_\ell) - \frac{\tau_\ell}{n}p^\ell = \frac{\xi_\ell}{n}.$$

Lemma 1. *For each $\ell \geq 0$ such that $p^\ell \| n$ we have $N(p^\ell) = \xi_\ell/n$.*

We will also prove another Lemma which we will require later. If p^ℓ is the abscissa of a vertex of the Newton polygon we have that the terms contributing to the coefficient of T^{p^ℓ} in the ramification polynomial give to the coefficient of T^{p^j} contributions having K-valuation at most $e_K(\ell - j)$ bigger, for $j < \ell$. In other words we have that $N(p^j) < e_K(\ell - j) + N(p^\ell)$, for each $j \leq \ell$. Considering the last vertex of one side of the Netwon polygon, and since for each ℓ the slope is equal to $-\tau_\ell/n$ in the interval $[p^\ell, p^{\ell+1}]$ and $N(p^\ell) < e_K + N(p^{\ell+1})$, we have that then τ_ℓ has to be at most $n\frac{e_K}{(p^{\ell+1}-p^\ell)} = e_L/(p^{\ell+1}-p^\ell)$. Hence we have

Lemma 2. *We have*

$$\xi_j \leq e_L(\ell - j) + \xi_\ell$$

for each $j < \ell$, and furthermore

$$\tau_\ell \leq e_L/(p^{\ell+1}-p^\ell)$$

for each ℓ.

We now study the points $(j, v_K(\Phi_j))$ coming from a monomial $\Phi_j T^j$ that may lie on the boundary of the Newton polygon of $\Phi(T) = \sum_{i=0}^n \Phi_i T^i$. We claim that either their ordinate j is a power of p, either $\gamma_1 \mid j$, and the latter is only possible when $\gamma_0 = n$ is not a power of p, so that γ_1 is the biggest power of p dividing n, and the polygon of $\Phi(T)$ has slope 0 in the interval $[\gamma_1, \gamma_0]$.

Indeed, for each ℓ we have

$$\Phi_{p^\ell} = \sum_{i=p^\ell}^{n} \binom{i}{p^\ell} f_i \pi^{i-n},$$

and since the summands have different valuations modulo n the valuation of Φ_{p^ℓ} has to be equal to the minimal valuation of such terms. For any integer r the terms $\binom{i}{r} f_i \pi^{i-n}$ contributing to Φ_r have valuation which is at least as big as the valuation of $\binom{i}{p^\ell} f_i \pi^{i-n}$ when $p^{\ell+1} \nmid r$, and strictly bigger if $p^\ell \nmid r$, so when $p^\ell \| r$ we have that $v_L(\Phi_r) \geq v_L(\Phi_{p^\ell})$ and $(r, v_K(\Phi_r))$ cannot be on the boundary of the polygon unless possibly when the segment containing p^ℓ has horizontal slope, $p^\ell = \gamma_1$ and $p^\ell \mid r$.

For integer $m \geq 0$ let's consider the polynomials

$$S_m(T) = \overline{\pi^{-n\phi_{L/K}(m)} \Phi(\pi^m T)}.$$

If $m \geq 1$, or n is a power of p, then $S_m(T)$ is of the form

$$S_m(T) = \sum_{i=a}^{b} c_i T^{p^i}$$

for some coefficients c_i, where $p^a = p^b = \gamma_i$ when m is not a ramification break and $m \in (t_{i+1}, t_i)$ say, while $\gamma_i = p^a$ and $\gamma_{i-1} = p^b$ if $m = t_i$ for some i. In particular they are additive polynomials.

On the other hand if $m = 0$ and n is not a power of p (and hence L has a non-trivial tamely ramified subextension) the terms appearing in $S_0(T) = \overline{\Phi(T)}$ are all coming from the leading monomial T^n, so that putting $n' = {}^n/_{\gamma_1}$ we have

$$S_0(T) = \sum_{j=1}^{n'} \binom{n}{\gamma_1 j} T^{\gamma_1 j}$$

$$= \sum_{j=1}^{n'} \binom{n'}{j} T^{\gamma_1 j}$$

$$= (1 + T^{\gamma_1})^{n'} - 1.$$

We collect these facts in the following proposition.

Proposition 2. *If $m \geq 1$ the polynomial $S_m(T)$ is an additive polynomial, which is composed by more than one monomial if and only if m is a lower ramification break. For $m = 0$ we have $S_0(T) = (1 + T^{p^s})^{n'} - 1$, where $n = p^s n'$ and $(p, n) = 1$.*

When the context is clear, we will abuse of notation and also denote by S_m the induced map $\theta \mapsto S_m(\theta)$ over the residue field or an extension thereof.

2.1. Change induced on the coefficients by a substitution.

We study now the effect of replacing the minimal polynomial $f(T)$ of π with the minimal monic polynomial $g(T)$ of a different uniformizer ρ.

Let's take $\rho = \pi + \theta \pi^{m+1} + \mathcal{O}(\pi^{m+2})$, we will identify the term $(f_i - g_i)\rho^i$ which has minimal valuation for general θ, and which gives information about the most significant change induced on the coefficients $f_i \to g_i$ as consequence of the substitution $\pi \to \rho$.

The non-zero terms $(f_i - g_i)\rho^i$ have valuations with different remainders modulo n, and furthermore we have

$$\sum_{i=0}^{n-1} (f_i - g_i)\rho^i = f(\rho) - g(\rho)$$

$$= f(\rho) = \pi^n \Phi(\theta \pi^m + \mathcal{O}(\pi^{m+1})),$$

considering the definition of ρ. If $m \geq 1$, being $\rho \equiv \pi \pmod{\mathfrak{p}_K^2}$ we obtain the following Lemma, after dividing by $\pi^{n(\phi_{L/K}(m)+1)}$ and reducing the expression modulo $\mathfrak{p}_K$.

Lemma 3. *If $m \geq 1$ and $g(T)$ is the minimal monic polynomial of an element of the form $\rho = \pi + \theta\pi^{m+1} + \mathcal{O}(\pi^{m+2})$ we have*

$$\overline{(f(\pi) - g(\pi)) \cdot \pi^{-n(\phi_{L/K}(m)+1)}} = S_m(\theta).$$

Since $n \mid v_L(f_i - g_i)$ for each i, the unique term $(f_i - g_i)\pi^i$ of $f(\pi) - g(\pi)$ which may be contributing to the left hand side is for i satisfying

$$i \equiv n(\phi_{L/K}(m) + 1) \pmod{n},$$

so i is uniquely determined being $0 \leq i < n$. We observe that if $m \geq 1$ is not a lower ramification break then S_m is surjective being κ_K finite and hence perfect, while if $m = t_i$ for some i then it may not be surjective, when the additive polynomial $S_{t_i}(T)$ has a root over the residue field κ_K.

Assume t_i to be an integer, we will later show that the polynomial $S_{t_i}(T)$ only depends on the field extension L/K and on the class of $\pi \mod \mathfrak{p}^2$, as a consequence of a stronger result, Theorem 2, which is proved independently. For the moment we can give a definition of reduced polynomial without assuming this invariance, even though the definition will be less manageable from a practical point of view.

Let I_m be the image of S_m, and also its preimage in $\mathcal{O}_L$ when the context is clear. Lemma 3 says that passing to the minimal polynomial of an element of the form $\pi + \theta\pi^{m+1} + \mathcal{O}(\pi^{m+2})$), if $n(\phi_{L/K}(m) + 1) = jn + i$ with $0 \leq i \leq n$, we can change the corresponding term f_i by an element of $\pi^{nj}I_m$ while all other terms $f_r\pi^r$ are unchanged modulo π^{jn+i+1}. Since the polynomials S_r for $r \leq m$ are certainly unchanged too, this observation motivates the following definition.

Definition 1. Let $f(x)$ be an Eisenstein polynomial, and assume each coefficient f_i to have an expansion

$$f_i = \sum_{j \geq 1}^{\infty} f_{i,j}\pi_K^j$$

with $f_{i,j} \in R$ for a fixed set of residue representatives R, and where π_K is a fixed uniformizer of K, and let $\bar{\eta}_f = \overline{-f_0/\pi_K}$. Assume the choice of a set $A_0 \subset \kappa_K^\times$ of representatives of $\kappa_K^\times/(\kappa_K^\times)^n$, and for each additive polynomial $S_m(T)$ for $m \geq 1$ a set of elements $A_m \subset \kappa_K$ which are representatives of the cokernel of the map $\theta \mapsto \eta_f^j S(\theta)$, where $j = [\phi_{L/K}(m) + 1]$.

We say that $f(x)$ is *reduced* (with respect to the choice of the A_i) when we have

(1) $\bar{\eta}_f = \overline{-f_0/\pi_K}$ is in A_0,
(2) for each $m \geq 1$, if $n(\phi_{L/K}(m) + 1) = jn + i$ for positive integers i, j with $i < n$, then we have $\overline{f_{i,j}} \in A_m$

We say that $f(x)$ is *reduced up to the level r* when condition 1 is satisfied, and condition 2 holds for all $m \leq r$.

If $f(T)$ is any Eisenstein polynomial, it's easy to see that the polynomial $\theta^n f(\theta^{-1}T)$ satisfies condition 1 for some suitable θ. A polynomial reduced up to level 0 can be obtained by the following algorithm.

Algorithm 1 Reduction (step 0)

$\bar{\alpha} \leftarrow \overline{-f_0/\pi_K}$,
$\bar{\beta} \leftarrow Representative(\bar{\alpha}, (\kappa_K^\times)^n)$,
$\bar{\theta} \leftarrow Solve(T^n = \bar{\beta}/\bar{\alpha})$,
$\theta \leftarrow Lift(\bar{\theta})$,
return $\theta^n f(\theta^{-1}T)$.

If i, j are as above, we have shown above $f_{i,j}\pi_K^j$ can be changed by any element in $\pi^{nj}I_m$ modulo π^{nj+1}, so $\overline{f_{i,j}}$ can be changed by any element of $\overline{(\pi^n/\pi_K)^j}I_m$. Since $\pi^n = -f_0 + \mathcal{O}(\pi^{n+1})$ we have that $\overline{(\pi^n/\pi_K)} = \bar{\eta}_f$, so $\overline{f_{i,j}}$ is changed by an element of $\bar{\eta}_f^j I_m$, and note that η_f is unchanged when passing to the minimal polynomial of an uniformizer of the form $\pi + \theta\pi^{m+1} + \mathcal{O}(\pi^{m+2})$), for a suitable θ.

In particular, if $f(x)$ is reduced up to the level $m-1$ we can obtain a polynomial reduced up to the level m via the following reduction step.

Algorithm 2 Reduction (step m)

$j \leftarrow \lfloor \phi_{L/K}(m) + 1 \rfloor$,
$i \leftarrow n \cdot \{\phi_{L/K}(m) + 1\}$,
$\bar{\alpha} \leftarrow \overline{f_{i,j}}$,
$\bar{\beta} \leftarrow Representative(\bar{\alpha}, \text{image}(\bar{\eta}_f^j S_m))$,
$\bar{\theta} \leftarrow Solve(\bar{\eta}_f^j S_m(T) = \bar{\alpha} - \bar{\beta})$,
$\theta \leftarrow Lift(\bar{\theta})$,
$F(T) \leftarrow T + \theta T^{m+1} + \{\text{any terms of degree} \geq m+2\}$,
return $Resultant_U(f(U), T - F(U))$.

Indeed, if $g(T)$ is the returned polynomial we have

$$\overline{(f_{i,j} - g_{i,j})\pi_K^j \pi^{i-n(\phi_{L/K}(m)+1)}} = \overline{(f_{i,j} - g_{i,j})}\bar{\eta}_f^{-j} = S_m(\bar{\theta}),$$

and consequently $\overline{g_{i,j}} = \bar{\beta} \in A_m$. Since we allow any higher order term in the choice of $F(T) = T + \theta T^{m+1} + \dots$, we anticipate that for a suitable $F(T)$ it will not be necessary to compute the resultant appearing in the algorithm as the determinant of a big matrix with coefficients in $K[T]$, see Remark 2.

Remark 1. *If m is bigger than the biggest lower ramification break t_k, then $S_m(x)$ is surjective, and the function $n(\phi_{L/K}(m)+1)$ assumes as possible values all integers $> n(\phi_{L/K}(t_k) + 1)$. Consequently we can arbitrarily change all the representatives $f_{i,j}$ whenever*

$$v_L(\pi_K^j \pi^i) = nj + i > n(\phi_{L/K}(t_k) + 1), \tag{1}$$

without affecting the generated extension, turning them all to 0 for instance. In this way we recover the well known quantitative criterion on the distance of two Eisenstein polynomials ensuring that they generate the same extension, as considered in [Kra62, PR01, Yos11].

2.2. **Characterizing reduced polynomials.** We start with a few remarks about Definition 1. Since we allow a different choice of the representing sets A_m for each m, where the 0 element of the image of the map is not even requested to be represented by 0, we have that each Eisenstein polynomial is reduced for a suitable choice of the A_m. While this choice is very far from what would be recommended in a computer algebra system it will be useful to be able to consider each Eisenstein polynomial as being already reduced.

On the other hand on a computer algebra system we can expect to have a more or less canonical way for selecting representing elements of a quotient, and selecting 0 as representative of the zero element in the quotient. Under this hypothesis we clarify here how a reduced polynomial looks like. In particular we will see that, for each $\ell \geq 0$ such that p^ℓ divides n, the possible valuations of the terms $f_{i,j}\pi_K^j\pi^i$ such $p^\ell\|i$ belong to one fixed interval, *with some exception*.

Fix ℓ and let us consider the terms $f_{i,j}\pi_K^j T^i$ with $p^\ell\|i$, we deduce a lower bound for the value of $nj + i$ from the shape of the Newton polygon of the ramification polynomial. Indeed, the contribution to the coefficient of T^{p^ℓ} in $\Phi(T)$ is

$$\pi^{-n} f_{i,j}\pi_K^j\pi^i \binom{i}{p^\ell},$$

and since the contributions coming from different monomials of $f(T)$ have different valuations modulo n then their smallest valuation should be at least $nN(p^\ell) = \xi_\ell$. In the same way we obtain that any term $f_{i,j}\pi_K^j T^i$ with $p^\ell\|i$ and $nj - n + i \geq \xi_\ell$ is compatible with the ramification data, and when $p^\ell\|\xi_\ell$ and p^ℓ is the abscissa of a vertex of the ramification polygon then there should be a term $f_{i,j}\pi_K^j T^i$ such that the valuation $nj - n + i$ of the contributed term is exactly ξ_ℓ, this case corresponds to a vertex of the Netwon polygon and hence the minimum is reached.

We will show now that starting all the terms $f_{i,j}\pi_K^j T^i$ with $p^\ell\|i$ and $nj + i$ big enough are turned to 0 by the reduction algorithm, with a few exceptions. Indeed, we claim that the integers which are multiple of p^ℓ and $> n\phi(\tau_\ell) = \sigma_\ell$ are all of the form $n\phi_{L/K}(m)$ for some $m > t_\ell$ (note that σ_ℓ may not be a multiple of p^ℓ itself, we are considering non-Galois extensions and t_r and $\phi(t_r)$ may not be integers).

To show the claim we work by induction on the number of ramification breaks. If $p^\ell < \gamma_{k-1}$ then $\tau_\ell = t_k$, and $nN(1)$ is certainly an integer being equal to $v_L(\mathscr{D}_{L/K})$, and $n\phi_{L/K}(m)$ for integer m assumes as values all integers which are $> n\phi_{L/K}(t_k)$, being $n\phi_{L/K}(x)$ equal to $nN(1) + x$ for integer $m > t_k$. Assume instead $p^\ell \geq \gamma_{k-1}$, then by induction $\frac{n}{\gamma_{k-1}}\phi_{K_{t_{k-1}^+}/K}(m)$ takes as values any multiple of p^ℓ/γ_{k-1} which is bigger than $\frac{n}{\gamma_{k-1}}\phi_{K_{t_{k-1}^+}/K}(\tau_\ell)$ for integer $m > \tau_\ell$. So $n\phi_{K_{t_{k-1}^+}/K}(x)$ satisfies the required property with respect to p^ℓ, and so does $n\phi_{L/K}(x)$ which is obtained as the minimum of $n\phi_{K_{t_{k-1}^+}/K}(x)$ and $nN(1) + x$.

Consequently we have from the claim that all the terms $f_{i,j}\pi_K^j$ with $p^\ell\|i$ and $nj - n + i \geq \sigma_\ell$ can be forced to satisfy $f_{i,j} = 0$, except possibly when $nj - n + i$ is itself equal to σ_r for some $r \leq \ell$, in this case we can only force $f_{i,j}$ to be a suitable representative depending on the image of the polynomial $S_{\tau_r}(T)$, which may not be surjective as a function over κ_K.

In the case of three breaks we have the following figure representing the values $nj - n + i$ of the terms of a reduced polynomial.
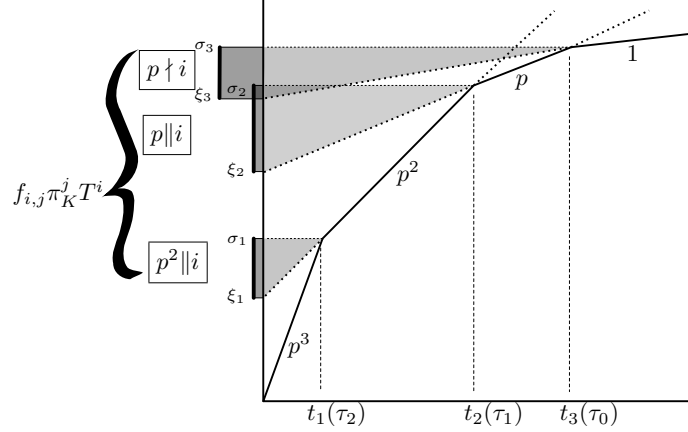
We state the above results in the following Proposition.

Proposition 3. *Let $f(x)$ be a reduced Eisenstein polynomial, and assume each coefficient f_i to have an expansion*

$$f_i = \sum_{j \geq 1}^{\infty} f_{i,j} \pi_K^j.$$

Assume $p^\ell \| i$, then $f_{i,j}$ is non-zero only when

$$\xi_\ell \leq nj - n + i < \sigma_\ell,$$

or when $nj - n + i$ is equal to some σ_r and the corresponding additive polynomial $S_{\tau_r}(T)$ has a root in κ_K.

In other words we have that starting from a certain points all terms $f_{i,j}\pi_K^j$ for $p^\ell \| i$ can all be simplified to 0, except at upper ramification breaks. We will later see how this phenomenon can be interpreted in terms of local class field theory for abelian extensions, or in connection with Serre mass formula [Ser78] in some simple particular case.

2.3. **Representation of automorphism as power series.** Applying such substitutions for increasing m we are taking into account all transformations $F(\pi)$ of π by a power series without constant coefficient $F(T) = \theta_1 T + \theta_2 T^2 + \dots$ which may provide an element whose minimal polynomial is reduced, because any such power series can be written as a composition of polynomials of the form $T(1 + \theta T^m)$. Applying the above reduction step for increasing m, when m is not equal to a ramification break t_i we have a unique possible choice for the class $\bar{\theta}$ of θ in the substitution $\pi \to \pi(1 + \theta \pi^m)$. When $m = t_i$ for some i, the choice for $\bar{\theta}$ is defined up to an element which is a root of $S_{t_i}(T)$, and taking into account representatives θ for all possible choices for $\bar{\theta}$ we can track all possible outputs. We can run this algorithm starting from the set $\{f(T)\}$ and replacing each polynomial with the set of all possible outputs, which may not be unique at the ramification breaks t_i, and do so up to the level t_k. After this last step we obtain reduced polynomials turning to 0 all the $f_{i,j}$ for i, j such that $nj + i > n(\phi_{L/K}(t_k) + 1)$.

Since some outputs may be repeated we end with a multiset of reduced polynomials. Clearly different power series $F(T)$, $G(T)$ may give the same value $F(\pi) = G(\pi)$ when evaluated in π, but we will show that we took into account all the different *values* $F(\pi) \in L$ such that the minimal polynomial of $F(\pi)$ is reduced.

Indeed, in step 0 we considered all possible values for $F(\pi)$ modulo $\mathfrak{p}_L^2$, and assume by induction that all the $F(\pi)$ taken in to account up to step $m - 1$ cover all possible values modulo $\mathfrak{p}_L^{m+1}$. The values $F(\pi) + \theta F(\pi)^{m+1} + \mathcal{O}(\pi^{m+2})$ covered in

---

Algorithm 3 All reduced polynomials

$\{t_1, \ldots, t_k\} \leftarrow LowerRamificationBreaks(f(T))$
$A \leftarrow \{f(T)\}$
for $m = 0 \to t_k$ **do**
    $B \leftarrow \emptyset$
    for $g(T) \in A$ **do**
        $B \leftarrow B \cup AllReductions(g(T), m)$
    end for
    $A \leftarrow B$
end for
$a \leftarrow [\phi_{L/K}(t_k) + 1]$
$b \leftarrow n \cdot \{\phi_{L/K}(t_k) + 1\}$
return $A \mod (\pi^{a+1}, \pi^a T^b)$

---

step m, for all admissible representatives θ, will provide all possible values modulo $\mathfrak{p}_L^{m+2}$.

Let $\rho_i(\kappa_K)$ be equal to the cardinality of $\kappa_K^\times/(\kappa_K^\times)^n$ if $t_i = 0$, and to be the number of roots of $S_{t_i}(x)$ contained in κ_K if $t_i > 0$. The cardinality of the multiset of polynomials obtained as output of the algorithm can be computed counting for each m the number of possible choices which is indeed equal to $\rho_m(\kappa_K)$, and the total cardinality is equal to the product of the $\rho_i(\kappa_K)$ over all i such that t_i is an integer, that is

$$B_{L/K} = \prod_{\substack{1 \le i \le k \\ t_i \in \mathbb{Z}}} \rho_i(\kappa_K).$$

We give now an interpretation of the $\rho_i(\kappa_K)$ as the number of automorphism of intermediate extensions. Indeed, if $t_i = 0$ then $\rho_i(\kappa_K)$ counts the number of n-th roots of the unity in κ_K, or equivalently of n'-th roots if $n = p^s n'$ with $(n', p) = 1$, which is also the number of automorphisms of a tame extension of degree n' of K, like K_{0^+}/K is.

For $t_i > 0$ let's consider the intermediate extension $K_{t_i^+}/K_{t_i}$: if $g(T)$ is the minimal polynomial of π over K_{t_i} (which is a factor of $f(T)$) then

$$\overline{\pi^{-n(\phi_{i-1}(t_i)+1)}g(\pi^{t_i+1}T + \pi)} = S_{t_i}(T),$$

and consequently representatives θ of the roots of $S_{t_i}(T)$ are exactly those such that

$$\sigma(\pi)/\pi = 1 + \theta\pi^{t_i} + o(\pi^{t_i})$$

for some K_{t_i}-automorphism $\sigma \in \mathrm{Aut}(L^{\mathrm{sep}}/K_{t_i})$. Now after extending the elements of $\Gamma_{t_i^+}$ to the normal closure we have $\Gamma_{t_i^+}(\sigma|_L) = \sigma\Gamma_{t_i^+}$, this is immediate considering $\Gamma_{t_i^+}$ as the image of elements of a ramification (normal) subgroup of a bigger Galois extension containing L. Consequently averaging over $\Gamma_{t_i^+}$ we obtain

$$\sigma(\pi_{K_{t_i^+}})/\pi_{K_{t_i^+}} = 1 + \theta^{\gamma_i}\pi_{K_{t_i^+}}^{t_i} + o(\pi_{K_{t_i^+}}^{t_i}),$$

where $\pi_{K_{t_i^+}} = N_{L/K_{t_i^+}}(\pi)$. The equality holds because t_i is smaller than the all ramification numbers of the extension $L/K_{t_i^+}$, by keeping into account the properties of the norm map $N_{L/K_{t_i^+}}$ (see [FV02, Chap. 3, §1, Prop. 1.5]).

If $\sigma(\pi_{K_{t_i^+}}) \in K_{t_i^+}$ then $\bar{\theta}$ is in κ_K, and on the other hand if $\bar{\theta} \in \kappa_K$ then $\sigma(\pi_{K_{t_i^+}})$ can be approximated better than any other conjugate of $\pi_{K_{t_i^+}}$ having $K_{t_i^+}/K_{t_i}$ only one ramification break, and consequently $\sigma(\pi_{K_{t_i^+}}) \in K_{t_i^+}$ by Krasner Lemma. In

other words we have one root of $S_{t_i}(T)$ in κ_K for each conjugate of $\pi_{K_{t_i^+}}$ contained in $K_{t_i^+}$, and $\rho_i(\kappa_K) = \# \operatorname{Aut}(K_{t_i^+}/K_{t_i})$.

So we have that $B_{L/K}$ is an invariant of the extension L/K. Considering the subgroups $\operatorname{Aut}(L/K_{t_i})$ of $\operatorname{Aut}(L/K)$ and the corresponding quotients as subgroups of $\operatorname{Aut}(K_{t_i^+}/K_{t_i})$, we observe that $B_{L/K}$ provides a "naive" upper bound to the cardinality of $\operatorname{Aut}(L/K)$, but which is in general tighter than the full degree $[L:K]$.

Let $f_1(x), \ldots, f_r(x)$ be all the reduced polynomials obtained applying the above algorithm. The number of times we obtain the same polynomial $f_i(x)$ is equal to the number of distinct $F_j(\pi)$ such that $f_1(F_j(\pi)) = 0$, and is consequently equal to the number of roots of $f_i(x)$ contained in L, in another words to the cardinality of $\operatorname{Aut}(L/K)$.

Theorem 1. *Each extension L/K is generated by a reduced polynomial, and the number of reduced polynomials generating a fixed extension L/K is*

$$B_{L/K}/\# \operatorname{Aut}(L/K).$$

If $f(x)$ is an Eisenstein polynomial such that a root generates an extension isomorphic to L, then the reduction algorithm outputs a multiset of cardinality $B_{L/K}$ formed by the reduced polynomials, each having multiplicity $\# \operatorname{Aut}(L/K)$.

We remark that if $F(T)$ is a power series such that $F(\pi)$ is a conjugate of π, the algorithm giving the set of special polynomials can collect all the θ used in the substitutions $\pi \to \pi + \theta\pi^{m+1}$ to produce an expression of

$$F(T) \mod (f(T), T^{t_k+1}),$$

which can be used to realize the group $\operatorname{Aut}(L/K)$ as group of truncated power series under composition, we omit the details of the construction.

Note that there is a unique reduced representative for Eisenstein polynomials generating Galois extensions, while in general we have a set of polynomials which is equal to the ratio of the "naive" bound on the number of automorphisms to the real number of automorphisms. We remark that extinguishing the redundancy from the above family of reduced polynomials seems to be at least as hard as computing the cardinality of the automorphism group. This can probably be done in a few particular cases, like for polynomials of degree p^2 over an unramifed extension of $\mathbb{Q}_p$, but depends indeed on a criterion to detect which extensions are Galois and to establish the cardinality of the group of automorphisms.

2.4. **Comparison with Amano polynomials and Serre mass formula.** We provide here some qualitative observation, without being completely rigorous. First, if the degree n is prime with p it's easy to say what are reduced polynomials, and they are all of the form $T^n + \theta\pi_K$ for some representative $\theta \in R$ such that $\bar{\theta} \in A_0$, where A_0 is the chosen set of representatives of $K^\times/(K^\times)^n$.

When $n = p$, Amano defined in [Ama71] a set of special generating polynomials composed by trinomials. The equations considered here turn out to look much more complicated "visually" because they are no longer trinomials, but the number of parameters is clearly the same, and nevertheless Amano polynomials do not seem to be easily generalizable to higher degree.

Reduced polynomials of degree p are of the form

$$T^p + \sum_{i=1}^{p} \left(\sum_{\substack{pj+i \geq (p-1)t+p \\ pj+i < pt+p}} f_{i,j}\pi_K^j \right) \cdot T^i + \pi_K \left(+f_{0,t+1}\pi_K^{t+1} \right),$$

for some ramification jump t such that either $t = {}^{pe_K}/_{p-1}$, either t is $< {}^{pe_K}/_{p-1}$ and $(p-1)t$ is an integer prime with p. Furthermore the term $f_{0,t+1}\pi_K^{t+1}$ is present only when t is an integer and the additive polynomial $S_t(T)$ has a root in κ_K, which is precisely the case of the extensions being Galois.

We remark that given an extension L/K of degree p, then in the Galois cyclic case the uniformizer π_K may not be a norm by class field theory, so in general an additional term is indeed required. On the other hand if L/K is not Galois then π_K is always in $N_{L/K}(L^\times)$.

We give one last interpretation of this fact, under the light of the proof of Serre "mass formula". Considering the map

$$\left\{\begin{array}{l}\text{uniformizers of ex-}\\\text{tensions of degree } p\end{array}\right\} \xrightarrow{\text{``minimal polynomial''}} \left\{\begin{array}{l}\text{Eisenstein polyno-}\\\text{mials of degree } p\end{array}\right\}$$

we have a p-to-1 correspondence between measure spaces, whose scaling factor turns out to be determined by the discriminant of the extensions as proven in [Ser78]. Let's restrict the map to the uniformizers of a fixed extension L/K in the algebraic closure, then either the extension is Galois and the map is still p-to-1, either the extension is not Galois and the map becomes 1-to-1, but in this case the image has bigger measure.

In other words, for fixed degree and restricting to extensions with a fixed discriminant, the smaller is the space of polynomials generating one fixed isomorphism class of extensions, the bigger will be the automorphism group of these extensions. When applying the reduction algorithm to a polynomial of degree p generating L/K, we have that when the unique ramification jump t is an integer and the additive polynomial $S_t(T)$ is not surjective we can do *less simplifications* to the coefficients of the Eisenstein polynomial. Since any Eisenstein polynomial generating L is a possible output of the reduction algorithm (for a suitable choice of the A_i) we have that the set of possible polynomials generating L turns out to be "smaller", and that L/K is Galois having some non trivial automorphism and degree p.

For higher degree, and in particular when there are more ramification breaks, it becomes difficult to generalize this observation, because a modification which appear to be trivial at the first order may actually provoke some change to the higher order terms in the expansions. This fact also justifies the claim that reducing the family to have exactly one polynomial for each isomorphism class appears to be at least as hard as the computation of the number of isomorphisms for the extension determined by one Eisenstein polynomial.

3. A criterion to rule out possible reductions

To complement the above reduction algorithm we give a synthetic criterion to exclude an Eisenstein polynomial from generating an extension of which we know the set of all the reduced polynomials. In particular given two polynomials $f(T)$ and $g(T)$ we can often rule out early the possibility that a sequence of substitutions $\pi \to \pi + \theta\pi^{m+1} + \mathcal{O}(\pi^{m+2})$, starting from level $m = r$ say, may transform the minimal polynomial $f(T)$ of π into the new minimal polynomial $g(T)$, without having to compute the complete reduction.

Let's consider the monomial $(f_i - g_i)\pi^i$ having smallest valuation, which determines the valuation of $f(\pi) - g(\pi)$, and assume its valuation to be equal to $v = n(\phi_{L/K}(r) + 1)$ for some real number r. Let's select sets of representatives A_m which make $g(T)$ reduced, then we say that $f(T)$ can be reduced to $g(T)$ *greedily* if $g(T)$ is a possible output of the reduction algorithm applied to $f(T)$ starting from step $m = r$. The proof of the following proposition is clear.

Proposition 4. *If r is not an integer than $f(T)$ cannot be reduced greedily to $g(T)$.*

We also have the following Proposition, whose proof is immediate as well.

Proposition 5. *If r is an integer equal to a lower ramification break and $\overline{(f_i - g_i)\pi^{i-v}}$ is not in the image of $S_{t_i}(T)$, then $f(T)$ cannot be reduced greedily to $g(T)$.*

These observations are well complemented by the following Proposition, which makes them particularly effective in the case of Galois extensions.

Proposition 6. *Assume that one of $f(T)$ or $g(T)$ is known to generate a Galois extension, then $f(T)$ and $g(T)$ generate the same extensions if and only if one polynomial can be greedily reduced to the other.*

Proof. For a suitable choice of representatives $g(T)$ is already reduced, and for Galois extensions there is only one reduced polynomial in view of Theorem 1, so applying greedily the reduction algorithm to $f(T)$ we obtain $g(T)$ as unique possible output. The other implication is clear. $\square$

In other words for Galois extensions if $g(T)$ can be obtained in some way from $f(T)$, then it can also be obtained in the greedy way.

When considering Galois extensions over $\mathbb{Q}_p$ the $S_{t_i}(T)$ are the zero map over the residue field $\mathbb{F}_p$, so if r is a ramification break then $f(T)$ and $g(T)$ certainly generate non-isomorphic extensions, and we essentially recovered the main result of [Yos11].

However, it is possible to give a deeper criterion, which is more selective than what it is possible by an inspection of $f(\pi) - g(\pi)$ at the first order.

Consider the range of monomials $f_{i,j}\pi_K^j T^i$ corresponding to one ramification break as described in Prop. 3, then the intuitive idea is that if we can obtain $f(T)$ from $g(T)$ applying reductions of parameter $m \geq r$ then the first r terms in each such interval must be equal, because such terms are not going to be changed by any reduction of order $\geq r$. Such ranges can be independently "brought up to the front" (with respect to the p-adic valuation) computing formally a ramification polynomial of $f(T) - g(T)$, and considering the coefficients of $T, T^p, T^{p^2}, \ldots$, as we can see observing the contributions to the coefficient of T^{p^ℓ} in the ramification polynomial. Consequently taking into account a ramification polynomial for $f(T) - g(T)$ provides a synthetic and effective formalism to describe how some sets of coefficients must be equal in order to be able to pass from $f(T)$ to $g(T)$ via reduction step.

What we are going to prove is closely related to what was done in [Hei96] and Theorem 4.6 in particular, and shares the philosophy that the sets of monomials $f_i T^i$ with a fixed valuation of i live an independent life from the other monomials, up to a certain extent, and that when a uniformizer is changed $\pi \to \pi + \theta\pi^{m+1} + \mathcal{O}(\pi^{m+2})$ the change induced on minimal polynomial satisfies a certain continuity (in [Hei96] a different kind of defining equation formed by a power series with coefficients in a set of representatives was used rather than Eisenstein polynomials, but the underlying principle is the same). From a more effective point of view, such a continuity provides an easily verifiable criterion to exclude a polynomial from generating one fixed extension, which is particularly effective in the case of Galois extensions thanks to Prop. 6. What we need seems not to follow directly from the results of [Hei96] and additional steps would be needed to switch to power series and back to Eisenstein polynomials, so we will avoid using the slightly cumbersome notation of [Hei96] and prove our result directly.

For integers $a \geq 0$ and w let's define P_{p^a}, resp. $P_{p^a}(w)$, as the module generated over $\mathcal{O}_K$ by the monomials cT^i such that $p^a \mid i$, resp. those monomials such that

additionally $v_L(c) + i \geq w$. If $cT^i \in P_{p^a}(w)$ for some w, than we have

$$c \left(T + \theta T^{m+1} + \mathcal{O}(T^{m+2}) \right)^i - cT^i \in \sum_{j=0}^{a} P_{p^j}(w + e_L(a - j) + p^j m) \qquad (2)$$

as we can verify at once expanding the left hand side. Furthermore if $g \in P_{p^a}(w)$ and $h \in P_{p^b}(z)$ than clearly we have $gh \in P_{p^{\min\{a,b\}}}(w + z)$.

Lets consider the ramification polygon $\Phi(T) = \pi^{-n} f(\pi T + \pi)$, then the coefficient of T^{p^a} is has valuation at least ξ_a. Assume $p^a \| i$, from a monomial $f_i T^i$ we have a contribution $\binom{i}{p^a} f_i \pi^{i-n} T^{p^a}$ to the coefficient of T^{p^a} in $\Phi(T)$, so $v_L(f_i) + i - n$ should be at least ξ_a, and consequently the monomial $f_i T^i$ is contained in $P_{p^a}(\xi_a + n)$, being $v_L(f_i) + i \geq \xi_a + n$.

Consequently we have obtained that

$$f(T) \in \sum_{j=0}^{s} P_{p^j}(\xi_j + n), \qquad (3)$$

where s is the biggest integer such that $p^s \mid n$ (recall that $\xi_s = 0$).

What observed above we obtain the following.

Proposition 7. *Let $F(T) = T + \theta_{m+1} T^{m+1} + \theta_{m+2} T^{m+2} + \ldots$, then*

$$f(T) \equiv f(F(T)) \quad \mathrm{mod} \sum_{j=0}^{s} P_{p^j}(\xi_j + n + p^j m). \qquad (4)$$

Proof. Let's consider $f(T) - f(F(T))$, we will show that a monomial $f_i T^i$, which is contained in $P_{p^a}(\xi_a + n)$ by (3) say, yield various terms each having valuation at least $\xi_j + n + p^j m$ and in P_{p^j}, for some $j < a$. But we obtain terms in $P_{p^j}(\xi_a + n + e_L(a - j) + p^j m)$ by (2), and $\xi_a + e_L(a - j) \geq \xi_j$ by Lemma 2. $\qquad \square$

Assume $\pi = F(\rho)$ for a root ρ of $g(T)$, we have now obtained a congruence property for the power series $f(F(T))$, which clearly satisfies $f(F(\rho)) = 0$. The minimal polynomial of ρ is clearly a factor of $f(F(T))$ of degree n, and observe that the valuation the coefficient of T^n is 0 while the constant term has valuation 1, so its Newton polygon has exactly one side of length n and slope $-1/n$. In particular $g(T)$ is obtained by the factorization along the Newton polygon, or equivalently collecting the roots with positive valuation, which is exactly what is provided by the p-adic Weierstrass preparation Theorem.

We will however show a reduction which allows to approximate the minimal monic polynomial of ρ starting from $f(F(T))$, and keeping the congruence (4). Let's start putting $h_1(T) = f(F(T))$, and consider the polynomial $H_1(T)$ obtained taking the monomials of degree $\geq n$ of $h_1(T) - T^n$. If $H(T) = 0$ then there is no such monomial, and $g(T)$ is a monic polynomial of degree n, which is Eisenstein being $F(\pi)$ a root.

Let cT^r a monomial of $H_1(T)$ which minimizes the quantity $v_L(c) + r$, and take the monomial with r as big as possible among those achieving the minimum of $v_L(c) + r$, which are in a finite number. In other words, we are considering the higher valuation F on $\mathcal{O}_L[[T]]$ where

$$F(cT^r) = (F_1(cT^r), F_2(cT^r)) = (v_L(c) + r, \; -r) \in \mathbb{Z}^2$$

and the elements of $\mathbb{Z}^2$ are ordered lexicographically, and we take cT^r to be the monomial of $H_1(T)$ which minimizes $F(cT^r)$.

Let's replace now $h_1(T)$ with the new polynomial

$$h_2 = h_1(T) - h_1(T) \cdot cT^{r-n} = h_1(T) \cdot \left(1 - cT^{r-n} \right).$$

We can see that applying iteratively such step i times that either the minimum of the quantity $v_L(c) + r$ for the monomials of degree $\geq n$ of $H_i(T)$ is increased, either is decreased the biggest degree of the monomials achieving the minimum. Since the whole computation is done in $\mathcal{O}_K[[T]]$ the latter can only happen a finite number of times, and such minimum is increased after a finite number of steps.

Algorithm 4 Lifting step

$H_i(T) \leftarrow \{\text{sum of monomials of degree} \geq n \text{ of } h_i(T) - T^n\}$
$cT^r \leftarrow (\text{monomial of } H_i(T) \text{ minimizing } F)$
return $h_i(T) \cdot (1 - cT^{r-n})$

After a sufficient number of iterations we can replace $h_i(T)$ with the polynomial $h(T)$ formed by T^n plus the monomials of degree $< n$ of $h_i(T)$, obtaining an Eisenstein polynomial such that $h(F(\pi))$ is arbitrarily small, so $h(T)$ is itself an arbitrarily good approximation of the minimal polynomial of $F(\pi)$.

We need to show that while the above procedure approximating $g(T)$ is carried on the congruence satisfied by $f(F(T))$ is preserved. Indeed, assume the congruence to be satisfied by $h_i(T)$ and assume $h_{i+1}(T) = h_i(T)(1 - cT^{r-n})$. Then $cT^r \in P_{p^\ell}(\xi_\ell + n + p^\ell m)$ for some ℓ, being cT^r a monomial of $H_i(T)$ and in view of the congruence which we assume to be satisfied by $f(T)$ and $h_i(T)$. Let bT^s be a monomial of $h_i(T)$, then $bT^s \in P_{p^k}(\xi_k + n)$ for some k by equation (3) and by the congruence satisfied by $h_i(T)$. If $k < \ell$ we have

$$bT^s \cdot cT^{r-n} \in P_{p^k}(\xi_k + n + \xi_\ell + n + p^\ell m - n) \subseteq P_{p^k}(\xi_k + n + p^k m),$$

while when $k \geq \ell$ we have

$$bT^s \cdot cT^{r-n} \in P_{p^\ell}(\xi_k + n + \xi_\ell + n + p^\ell m - n) \subseteq P_{p^\ell}(\xi_\ell + n + p^\ell m).$$

We obtained that subtracting $h_i(T) \cdot cT^{r-n}$ from $h_i(T)$ preserves the congruence. Considering also an analogue of a ramification polynomial for $f(T) - g(T)$ we have the following Theorem.

Theorem 2. *Let $f(T)$ be an Eisenstein polynomial of degree n and π a root, if $g(T)$ is another Eisenstein polynomial of degree n having $\rho \in K(\pi)$ as root, and $\pi = \rho + \theta\rho^{m+1} + \mathcal{O}(\rho^{m+2})$ then we have that*

$$f(T) \equiv g(T) \mod \sum_{j=0}^{s} P_{p^j}(\xi_j + n + p^j m),$$

and the polynomial

$$f(\pi + \pi T) - f(\pi) - g(\pi + \pi T) + g(\pi)$$

has its Newton polygon contained in the Newton polygon of $f(\pi + \pi^{m+1}T)$.

Proof. We only need to prove the second assertion, but if cT^r is in $P_{p^j}(\xi_j + n + p^j m)$ then for each $k \leq j$ the contribution of $c(\pi + \pi T)^r$ to the coefficient of T^{p^k} has valuation at least $\xi_j + n + p^j m + (j - k)e_L$, which is at least $\xi_k + n + p^k m$ as shown above. $\qquad\square$

Remark 2. *We point out that the algorithm used during the proof to recover (an approximation of) the minimal polynomial of $\rho = F^{-1}(\pi)$ can be used to produce the minimal polynomial of a uniformizing element obtained deforming π in a much quicker way than by computing a resultant $Res_U(g(U), T - (U + \theta U^{m+1}))$ as the determinant of a $(n+m) \times (n+m)$ matrix with coefficients in $\mathcal{O}(T)$. Consequently taking $F(T) = T - \theta T^{m+1}$ and computing via the above approximation the minimal polynomial of the uniformizer ρ such that $\pi = \rho - \theta\rho^{m+1}$, we obtain the minimal*

polynomial of a uniformizer $\rho = \pi + \theta\pi^{m+1} + \mathcal{O}(\pi^{m+2})$, and this observation allows to exploit the free choice of $F(T)$ in Algorithm 2 to avoid the computation of the resultant.

4. Construction of totally ramified class fields

In this section we show how it is possible to convert a norm subgroup, representing a totally ramified abelian extension via local class field theory, into the unique reduced Eisenstein polynomial generating the extension.

We suppose given a finite index closed subgroup $N \subset K^\times$ such that $NU_{0,K} = K^\times$, so that the corresponding extension by local class field theory is totally ramified. Being closed we have $N \supset U_u$ for u sufficiently big, this hypothesis is automatically satisfied when K is a finite extension of $\mathbb{Q}_p$ and N has finite index.

We assume N to be described by a set of linear maps, one for each upper ramification break. That is for all $u \geq 0$ such that $U_{u,K} \not\subseteq NU_{u+1,K}$ we assume given a surjective homomorphism

$$\nu_u : NU_{u,K} \to V_u$$

having kernel exactly equal to $NU_{u+1,K}$, for some abstract group V_u which is naturally an $\mathbb{F}_p$-vector space for $u \geq 1$. Take ν_u to be the trivial map to the trivial group 1 when u is not an upper break, that is $NU_{u,K} = NU_{u+1,K}$. Note that the knowledge of all the maps ν_u determines uniquely the group N.

The map ν_0, when non-trivial, gives a condition on the representative $f_{0,1}$, or equivalently on the residue class $\overline{f_0/\pi_K}$, this correspond to the well known explicit description of local class field theory for tamely ramified extensions. On the other hand the terms appearing in a reduced polynomial in connection to the cokernels of the polynomials $S_{t_i}(T)$ attached to the lower breaks t_i are all of the form $f_{0,j}\pi_K^j$, because the upper breaks are integers by Hasse-Arf Theorem.

Consequently the choice of such representatives $f_{0,j}$ is determined by the condition that f_0 should be a norm from the extension determined by N, and a suitable f_0 can be selected changing appropriately π_K.

The ramification data is described by the upper breaks $u \geq 1$ and the dimensions of the corresponding V_u. Consequently after selecting f_0 we have fixed a skeleton for the reduced Eisenstein polynomial, formed by a well defined set of terms $f_{i,j}\pi_K^j T^i$, for $i \neq 0$, where the $f_{i,j}$ will be considered as unknowns in the set of representatives R. We will describe how it is possible to recover the $f_{i,j}$ from the maps ν_u.

The terms $f_{i,j}$ in a fixed range as in Prop. 3 can be evaluated at the level σ_ℓ when $p^\ell\|i$ say, making use the map $\nu_{\sigma_\ell/n-1}$ as we will now show. If m is such that $nj + i + p^\ell m = n\sigma_\ell + n$ it will be possible to describe the dependence of $N_{K(\pi)/K}(1 - \theta\pi^m)$ on the coefficient $f_{i,j}$ at the first order, obtaining a linear system from $\nu_{\sigma_\ell/n-1}$.

Definition 2. If $p^{\ell+1}|n$, we define R_ℓ to be the set of pairs (i,j) such that $j \geq 1$, $0 \leq i < n$, $p^\ell\|i$ and

$$\xi_\ell + n \leq nj + i < \sigma_\ell + n.$$

We assume R_ℓ to be ordered depending on the value of $nj + i$. We define $M(i,j)$ to be the number m such that

$$nj + i + p^\ell m = \sigma_\ell + n.$$

We remark that if the extension is abelian then $n|\sigma_\ell$ by Hasse-Arf theorem, so the m defined above is always an integer $\leq \tau_\ell$ and prime with p.

4.1. **Dependence of norms on a** $f_{i,j}$. We will now track the dependence of a norm $N_{K(\pi)/K}(1 - \theta\pi^m)$ on a representative $f_{i,j}$ appearing in the expansion of a coefficient. To do so, let's treat $f_{i,j}$ as an indeterminate, and apply a sufficient number of steps of Algorithm 4 to pass from $f(T + \theta T^{m+1})$ to the minimal polynomial $g(T)$ of ρ, where $\pi = \rho + \theta\rho^{m+1}$.

We clearly have $\rho = \pi - \theta\pi^{m+1} + \mathcal{O}(\pi^{m+2})$, and g_0/f_0 will be the norm of some element which is $1 - \theta\pi^m + \mathcal{O}(\pi^{m+1})$. Since we will obtain that the changes induced changing $f_{i,j}$ on all $N_{K(\pi)/K}(1 - \theta\pi^r + \mathcal{O}(\pi^{r+1}))$ for $r > m$ will be even smaller p-adically, this makes possible to ignore the $\mathcal{O}(\pi^{m+1})$.

In the expansion of $f(T + \theta T^{m+1})$ a term $f_{i,j}\pi_K^j(T + \theta T^{m+1})^i$ appears, and it has $f_{i,j}\pi_K^j T^i$ as main term. In the algorithm we start with $h_0(T) = f(T + \theta T^{m+1})$, and at the i-th step we subtract $h_i(T) \cdot cT^{r-n}$ from $h_i(T)$ for a monomial cT^{r-n} in $P_{p^k}(\xi_k + p^k m)$ for some $k \leq s$. From the monomial $f_{i,j}\pi_K^j T^i$ the other terms in $f_{i,j}$ which may appear in the algorithm have coefficient with valuation at least

$$nj + i + \min_{0 \leq k \leq s} \{\xi_k + p^k m\} = nj + i + n\phi_{L/K}(m),$$

where we are considering the mixed valuation $F_1(\pi_K^a T^b) = na + b$ on $\mathcal{O}_L[[T]]$.

Note that the minimum of $\xi_k + p^k m$ is obtained as the minimum of the piecewise linear function $nN(x) + mx$, which is $n\phi_{L/K}(m)$ in view of what proved before Proposition 1. We will denote for convenience this quantity as

$$A_{i,j}(m) = nj + i + n\phi_{L/K}(m).$$

The term $f_{i,j}\pi_K^j T^i$ is the main term coming from $f_{i,j}\pi_K^j(T + \theta T^{m+1})^i$, and the second contribution can be found considering the expansion

$$(1 + \theta T^m)^i = 1 + \binom{i}{p^\ell}(\theta T^m)^{p^\ell} + \binom{i}{p^\ell - 1}(\theta T^m)^{p^{\ell-1}} + \dots.$$

Putting as usual $p^\ell \| i$, we denote the valuation of the second term as

$$B_{i,j}(m) = nj + i + \min_{0 \leq k \leq \ell} \{e_L(\ell - k) + p^k m\}.$$

Such term is equal to

$$\binom{i}{p^\ell}\pi_K^j T^i \cdot (\theta T^m)^{p^\ell}$$

as long as $mp^\ell < e_L + mp^{\ell-1}$, that is $m < e_L/(p^\ell - p^{\ell-1})$, and if $m \leq M(i,j) \leq \tau_\ell$ this condition is certainly satisfied because

$$m \leq \tau_\ell \leq e_L/(p^{\ell+1} - p^\ell)$$

by Lemma 2.

By Proposition 3 we can assume $\ell < s$, and if $m \leq \tau_\ell$ we always have

$$B_{i,j}(m) = nj + i + p^\ell m < A_{i,j}(m).$$

So the main contribution to $N_{K(\pi)/K}(1 - \theta\pi^m) = g_0/f_0$ originated from $f_{i,j}\pi_K^j T^i$ is only coming from $f_{i,j}\binom{i}{p^\ell}\pi_K^j T^i \cdot (\theta T^m)^{p^\ell}$.

When $m = M(i,j)$ we obtain a condition on $f_{i,j}$ to have $N_{K(\pi)/K}(1 - \theta\pi^m)$ in the norm group for each θ, which can be used to determine the representative $f_{i,j}$.

This can be made to work when only one representative $f_{i,j}$ is unknown, but a more refined study is needed if we have to determine them all. In particular, we will see that there exists an ordering of such unknowns that allows to determine them all inductively. What complicates this idea is that it turns out to be necessary to interleave in a suitable way the ranges of representatives considered in Prop. 3.

It will be convenient to write down a comfortable lower bound for the functions $A_{i,j}$ and $B_{i,j}$ to ensure that the value of a particular representative $f_{i,j}$ has no

influence on $N_{K(\pi)/K}(\pi - \theta\pi^{m+1})$ modulo a suitable power of π. In particular we have that they are all bounded by

$$C_{i,j}(m) = nj + i + \min_{0 \le k \le \ell} \left\{ \xi_k - \xi_\ell + p^k m \right\},$$

where $\ell = v_p(i)$ as usual. We resume the properties proved in the following Lemma.

Lemma 4. *Denote with π a root of $f(T)$, and let $(i,j) \in R_\ell$. Then, for each $\theta \in U_K$, the value of*

$$N_{K(\pi)/K}(1 - \theta\pi^m) \mod \mathfrak{p}_K^u$$

does not depend on $f_{i,j}$, whenever u is $\le C_{i,j}(m)/n - 1$. Furthermore if $m = M(i,j)$ then $C_{i,j}(m) = \sigma_\ell + n$, and putting $u = C_{i,j}(m)/n - 1 = \phi_{L/K}(\tau_\ell)$ we have

$$N_{K(\pi)/K}(1 - \theta\pi^m) = N_{K(\pi_0)/K}(1 - \theta\pi_0^m) + \pi_K^u f_{i,j} \lambda_{i,j} \theta^{p^\ell} + \mathcal{O}(\pi_K^{u+1}), \quad (5)$$

where $\lambda_{i,j}$ is a fixed unit defined as

$$\lambda_{i,j} = \binom{i}{p^\ell} \cdot (-f_0/\pi_K)^{(i+p^\ell m)/n - 1},$$

and we set π_0 to be a root of the polynomial obtained from $f(T)$ setting $f_{i,j}$ to 0.

Proof. We just have to prove the (5). For $m = M(i,j)$ the variation of the constant term comes from the monomial $f_{i,j}\binom{i}{p^\ell}\pi_K^j T^i \cdot (\theta T^m)^{p^\ell}$ in the expansion of $f(T + \theta T^{m+1})$, and during the reduction each T^n is transformed into $-f_0$. Dividing by f_0 we obtain that the variation for $N_{K(\pi)/K}(1 - \theta\pi^m)$, which modulo π_K^{u+1} is

$$f_{i,j}\pi_K^j \binom{i}{p^\ell}(-f_0)^{(i+p^\ell m)/n - 1}\theta^{p^\ell} = \pi_K^u f_{i,j}\lambda_{i,j}\theta^{p^\ell}. \qquad \square$$

We will now assume that some $f_{i,j}$ have been determined and some not yet, and will show that it is possible to determined some of the unknown ones. For ℓ such that $p^{\ell+1} \| n$, consider the range of terms R_ℓ like in Prop. 3, and let (i_ℓ, j_ℓ) be the smallest pair $(i,j) \in R_\ell$ (i.e. the pair in R_ℓ with $nj + i$ as small as possible) such that the corresponding $f_{i,j}$ has not been identified yet.

We first prove a couple of technical lemmas about the functions $C_{i,j}(x)$.

Lemma 5. *The functions $C_{i,j}(x)$ are strictly increasing, and for $(i,j) \ne (i',j')$ then the functions $C_{i,j}(x)$ and $C_{i',j'}(x)$ are always different except possibly at one point. The difference $C_{i,j}(x) - C_{i',j'}(x)$ is constant when $v_p(i) = v_p(i')$, and $C_{i',j'}(x)$ can surpass $C_{i,j}(x)$ only when $v_p(i') > v_p(i)$.*

Proof. Follows directly from the definition. $\qquad \square$

Lemma 6. *Let $\Pi_L(x)$ be the real function $x \mapsto \min\{px, x + e_L\}$, and let $\Pi^{[h]}$ denote the h-times composition. Then if $y = C_{i,j}(m) - n$, for $(i,j) \in R_\ell$ and some $m \in \mathbb{N}$, then we have*

$$\Pi^{[h]}(y) \ge C_{i,j}(p^h m) - n,$$

for each $h \ge 1$.

Proof. It's enough to prove that $\Pi(y) \ge C_{i,j}(pm) - n$, and we can do so proving that both py and $y + e_L$ are bigger. This follows easily from the definition and from Lemma 2. $\qquad \square$

Let $K(x)$ be the function defined as

$$K(x) = \min_{0 \le \ell < s} C_{i_\ell, j_\ell}(x), \quad (6)$$

it is again a strictly increasing function which for each m describes up to which precision we can compute $N_{K(\pi)/K}(\pi - \theta\pi^{m+1})$, with the given information about the coefficients of $f(T)$.

Let I_ℓ be the set of real x where $K(x) = C_{i_\ell,j_\ell}(x)$, since two functions $C_{i,j}(x)$ can only cross once we have that I_ℓ is a (possibly infinite) topologically closed real interval, and taking into account the conditions under which a surpass may happen of Lemma 5 we obtain that I_k lies before I_ℓ if $k > \ell$. Let's merge in a unique bigger interval the I_ℓ such that the value of τ_ℓ is the same, and let J_r be formed by the union of the I_ℓ such that $\tau_\ell = t_r$. Let's also put $k_r = K^{-1}(n\phi(t_r) + n)$ for each r, then k_r is contained in the *interior* of J_r for some r, thanks to the following Lemma.

Lemma 7. *Let $A_1, \ldots, A_m$ be a sequence of intervals with extrema $\mathbb{R} \cup \{\pm\infty\}$, such that A_{i+1} begins exactly where A_i ends. Let $a_1 < a_2 < \cdots < a_m$ be real numbers contained in the interior of $\bigcup_{i=1}^m A_i$. Then a_i is contained in the interior of A_i, for some $1 \le i \le m$.*

Proof. The thesis is trivial when $m = 1$. If $m > 1$, then either a_m is in the interior of A_m, either we have that $a_1, a_2, \ldots, a_{m-1}$ are contained in the interior of $\bigcup_{i=1}^{m-1} A_i$ and the thesis follows by induction. $\square$

So, let r be such that k_r is in the interior of J_r, and let $L_1 \le L_2$ be the integers such that $\tau_\ell = t_r$ if and only if $\ell \in [L_1, L_2]$. Then we have that $C_{i_\ell,j_\ell}(k_r)$ is at least $n\phi_{L/K}(t_r) + n$ for $\ell \in [L_1, L_2]$, and strictly bigger for $\ell \notin [L_1, L_2]$. Put $m = k_r$.

For $L_1 \le \ell \le L_2$ let's redefine (i_ℓ, j_ℓ) to be the unique pair (i, j) in R_ℓ that $C_{i,j}(m) = n\phi_{L/K}(t_r) + n$. Then some pairs (i_ℓ, j_ℓ) will be unchanged while some others may be set to correspond to representatives f_{i_ℓ,j_ℓ} which are already known. This makes no harm since all these representatives will now be determined simultaneously. Since the equality need to hold already for some of the original (i_ℓ, j_ℓ) we obtain that $m = M(i_\ell, j_\ell)$ is an integer $< \tau_\ell = t_r$ and prime with p.

Let's consider the terms $f_{i_\ell,j_\ell} \pi_K^{j_\ell} T^{i_\ell}$ for ℓ in the given range, and lets vary the f_{i_ℓ,j_ℓ}. Put $u = \phi_{L/K}(t_r)$.

Lemma 8. *If the $f_{i,j}$ already known were determined inductively we already have*
$$N_{K(\pi)/K}(1 - \theta\pi^m) \in U_u N,$$
and the class modulo $U_{u+1}N$ only depend on $\bar{\theta}$.

Proof. Indeed let $u' = \phi_{L/K}(t_{r'}) \le u$ be an upper ramification jump and $m' \ge m$, and assume at least one of these inequality to be strict. We will show that there was a previous step where we computed some currently known coefficient, by requesting $N_{K(\pi)/K}(1 - \theta\pi^{m'})$ to be in $U_{u'+1}N$ for each θ.

If $\phi_{L/K}(m') > u'$ then we always have $N_{K(\pi)/K}(1 - \theta\pi^{m'}) \in U_{u'+1}$, by the properties of the norm map [FV02, Chap 3, Prop 3.1]. Consequently assume $\phi_{L/K}(m') \le u'$, or $m' \le \psi_{L/K}(u') = t_{r'}$ applying $\psi_{L/K}$. If $(m, p) = 1$, let $[L_1', L_2']$ be the interval of possible ℓ such that $\tau_\ell = t_{r'} \ge m$, and for each ℓ we have a pair (i_ℓ', j_ℓ') for $L_1' \le \ell \le L_2'$ which has the property that $m' = M(i_\ell', j_\ell')$, and $C_{i_\ell',j_\ell'}(m') = nu' + n \le K(m)$. Thus the $C_{i_\ell',j_\ell'}(x)$ is certainly not $\ge K(x)$ and cannot appear in the (6). This means that the $f_{i_\ell',j_\ell'}$ for $L_1' \le \ell \le L_2'$ have been determined at a previous step, where we guaranteed that $N_{K(\pi)/K}(1 - \theta\pi^{m'}) \in U_{u'+1}$.

When $p | m$ let's consider the elements of the form $(1 + \theta\pi^{m''/p^w})^{p^w}$ as generators of $U_{m'}/U_{m'+1}$ (see [FV02, Chap. 1, Prop. 5.7]), and note that $m' \lesssim pe_L/(p-1)$). We are done if we show that $N(1 + \theta\pi^{m''}) \in NU_{u''+1}$ for $m'' = m'/p^w$ and each upper break $u'' \le \Pi_K^{[-w]}(u')$, where $\Pi_K(x) = \min\{px, x + e_K\}$.

We can assume $m'' \le \psi_{L/K}(u'') = t_{r''}$ as above. Consider as above an ℓ such that $\tau_\ell = t_{r''} = \psi_{L/K}(u'')$, and a pair $(i_\ell'', j_\ell'') \in R_\ell$ with $m'' = M(i_\ell'', j_\ell'')$. Then $C_{i_\ell'',j_\ell''}(m'') = nu'' + n$, and $C_{i_\ell'',j_\ell''}(m')$ is certainly $\le \Pi_L^{[w]}(nu'') + n \le nu' + n$ by

Lemma 6. We have that $C_{i''_\ell, j''_\ell}(x)$ is not $\geq K(x)$, and the condition $N(1+\theta\pi^{m''}) \in NU_{u''+1}$ was verified in a previous step. $\qquad\square$

We have from the Lemma 4, applied once for each pair (i_ℓ, j_ℓ) for $L_1 \leq \ell \leq L_2$, that changing the f_{i_ℓ, j_ℓ} we have

$$N_{K(\pi)/K}(1 - \theta\pi^m) = N_{K(\pi_0)/K}(1 - \theta\pi_0^m) + \sum_{\ell=L_1}^{L_2} \pi_K^u f_{i_\ell, j_\ell} \lambda_{i_\ell, j_\ell} \theta^{p^\ell} + \mathcal{O}\left(\pi^{u+1}\right),$$

where π_0 is the root of the polynomial with the unknown f_{i_ℓ, j_ℓ} all set to 0.

Now for some choice of the f_{i_ℓ, j_ℓ} we want $N_{K(\pi)/K}(1 - \theta\pi^m)$ be in the kernel of $\nu_u : NU_u/NU_{u+1} \xrightarrow{\sim} V_u$, for each residue representative θ. The condition only depends on the reductions $\bar{\theta}$ and $\overline{f_{i_\ell, j_\ell}}$ and is $\mathbb{F}_p$-linear in them, so we can impose it to hold only for a set of values for $\bar{\theta}$ which generate κ_K over $\mathbb{F}_p$. Let $\bar{\alpha}_1, \ldots, \bar{\alpha}_F$ be such a basis, then we can decompose each

$$\overline{f_{i_\ell, j_\ell}} = \sum_{k=1}^{F} \overline{f_{i_\ell, j_\ell, k}} \bar{\alpha}_k$$

and consider $\overline{f_{i_\ell, j_\ell, k}}$ as unknown over $\mathbb{F}_p$.

Fix a lifting $\alpha_k \in \mathcal{O}_K$ for each $\bar{\alpha}_k$, we have an equation

$$\nu_u(N_{K(\pi_0)/K}(1 - \alpha_k\pi_0^m) + \sum_{\ell=L_1}^{L_2} \pi_K^u \left[\sum_{k=1}^{f} f_{i_\ell, j_\ell, k}\alpha_k\right] \lambda_{i_\ell, j_\ell} \alpha_k^{p^\ell}) = 0$$

in V_u for each generator $\bar{\theta} = \bar{\alpha}_k$. The codomain V_u has $\mathbb{F}_p$-dimension equal to the "multiplicity" of the ramification jump $\Lambda = L_2 - L_1 + 1$. So we have an inhomogeneous system formed by $F \cdot \Lambda$ equations over $\mathbb{F}_p$, for the same number of unknowns $\overline{f_{i_\ell, j_\ell, k}}$.

Consequently we have a unique solution for the $\overline{f_{i_\ell, j_\ell, k}}$ if we can prove that the system is non-degenerate. We can equivalently prove that the connected homogeneous system

$$\nu_u\left(1 + \sum_{\ell=L_1}^{L_2} \pi_K^u \left[\sum_{k=1}^{f} f_{i_\ell, j_\ell, k}\alpha_k\right] \lambda_{i_\ell, j_\ell} \theta^{p^\ell}\right) = 0, \qquad \text{for all } \theta$$

has no non-trivial solution. Subtracting 1 and dividing by a suitable power of π_K, the system can be interpreted as the request that the additive polynomial

$$\sum_{\ell=L_1}^{L_2} \overline{f_{i_\ell, j_\ell} \lambda_{i_\ell, j_\ell}} \bar{\theta}^{p^\ell}$$

in $\bar{\theta}$ should have range identically contained in a subspace of codimension $L_2 - L_1 + 1$. Since the powers of $\bar{\theta}$ appearing are p-th powers ranging from p^{L_1} to p^{L_2}, we have that its corank as linear map is at most $L_2 - L_1$ (see [FV02, Chap. 5, §2]). Consequently such a non-trivial solution of the homogeneous system is impossible, and the original system is non-degenerate.

Theorem 3. *Given a closed finite index subgroup $N \subset K^\times$ corresponding to a totally ramified class field, there exists an ordering of the representatives $f_{i,j}$ appearing in the expansion of the coefficients of a generic Eisenstein polynomial which allows to determine the coefficients of the reduced Eisenstein polynomial generating the extensions corresponding to N.*

It is indeed clear that the above procedure where the $f_{i,j}$ are obtained solving linear equations can be converted into an algorithm to construct explicitly a minimal equation corresponding to a class field. The $f_{i,j}$ allowed by the ramification data

but with $(i,j) \notin R_\ell$ for each ℓ can be assumed to be all 0, or set to any arbitrary value (indeed, they are exactly those set by the reduction algorithm). On the other hand, during the construction we guarantee that for each $m > 0$ and prime with p, and for each θ, we have $N_{K(\pi)/K}(1 - \theta\pi^m) \in N$, because the condition $\nu_u(N_{K(\pi)/K}(1 - \theta\pi^m)) = 0$ is verified for all u at some point of the algorithm, implying that all norms are contained in N.

Remark 3. *We observe that this construction produces an alternative and constructive proof of the Existence Theorem of class field theory for totally ramified extensions, because for each finite index closed subgroup N of $K^\times$ with index n we construct an extensions of degree n having norm subgroup contained in N. We can construct precisely one reduced polynomial of degree $(K^\times : N)$ for each N, and considering all possible reduction steps we have easily that the group of norms has to be exactly equal to N, and that all intermediate fields $K_{t_r^+}/K_{t_r}$ are Galois, so the generated field L/K has to be Galois by Theorem 1.*

It would be interesting to extend this construction to recover the Artin map from $K^\times/N$ to $\mathrm{Gal}(K/L)$, proving that these two groups are indeed isomorphic and describing explicitly the isomorphism. The above methods do not even give an easy proof that the extension obtained is abelian, without assuming local class field theory.

REFERENCES

[Ama71] Shigeru Amano, *Eisenstein equations of degree p in a $\mathfrak{p}$-adic field*, J. Fac. Sci. Univ. Tokyo Sect. IA Math **18** (1971), 1–21.

[Del84] Pierre Deligne, *Les corps locaux de caractéristique p, limites de corps locaux de caractéristique* 0, Representations of reductive groups over a local field, Travaux en Cours, Hermann, Paris, 1984, pp. 119–157.

[FV02] Ivan Borisovich Fesenko and Sergei Vladimirovich Vostokov, *Local fields and their extensions*, American Mathematical Society, 2002.

[Hei96] Volker Heiermann, *De nouveaux invariants numériques pour les extensions totalement ramifiées de corps locaux*, Journal of Number Theory **59** (1996), no. 1, 159–202.

[Hel91] Charles Helou, *On the ramification breaks*, Communications in Algebra **19** (1991), no. 8, 2267–2279.

[Kra62] Marc Krasner, *Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique*, C. R. Acad. Sc. Paris **254** (1962), 3470–3472, *Ibidem* 255:224–226, 1682–1684, 2342–2344, 3095–3097, 1962.

[Li97] Hua-Chieh Li, *p-adic power series which commute under composition*, Transactions of the American Mathematical Society **349** (1997), no. 4, 1437–1446.

[Lub81] Jonathan Lubin, *The local Kronecker-Weber theorem*, Transactions of the American Mathematical Society **267** (1981), no. 1, 133–138.

[Pau06] Sebastian Pauli, *Constructing class fields over local fields*, Journal de théorie des nombres de Bordeaux **18** (2006), no. 3, 627–652.

[PR01] Sebastian Pauli and Xavier-François Roblot, *On the computation of all extensions of a p-adic field of a given degree*, Mathematics of Computation **70** (2001), no. 236, 1641–1660.

[Ser78] Jean-Pierre Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C.R. Acad. Sci. Paris Sér. A-B **286** (1978), 1031–1036.

[Ser79] ———, *Local fields*, Springer, 1979.

[Yam68] Sunao Yamamoto, *On a property of the Hasse's function in the ramification theory*, Memoirs of the Faculty of Science, Kyushu University. Series A, Mathematics **22** (1968), no. 2, 96–109.

[Yos11] Manabu Yoshida, *An ultrametric space of Eisenstein polynomials and ramification theory*, Arxiv preprint arXiv:1105.5221 (2011).

E-mail address: `maurizio.monge@sns.it`

SCUOLA NORMALE SUPERIORE DI PISA - PIAZZA DEI CAVALIERI, 7 - 56126 PISA